Nowhere to Hide

The Growing Threat to Air Bases

Col Shannon W. Caudill, USAF
Maj Benjamin R. Jacobson, USAF

Wearing US Army uniforms, the attackers penetrated the air base's defenses under the cover of night. Armed with rifles, rocket-propelled grenade launchers, and suicide vests, the 14-man team began its deadly mission against an air base in Helmand Province, Afghanistan, jointly manned by the North Atlantic Treaty Organization's (NATO) International Security Assistance Force (ISAF). Hours of combat ensued, and the morning light revealed the destruction of six AV-8B Harrier jets and damage to two other aircraft; additionally, "six aircraft hangers [*sic*] suffered damage," and "six refueling stations were destroyed."[1] In the aftermath, 14 insurgents and two US Marines lay dead while eight coalition military members and one contractor were wounded. In September 2012, this insurgent operation constituted the most successful ground attack against NATO's ISAF air assets to date in the Afghanistan conflict.

Italian general Giulio Douhet famously noted that "it is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air."[2] Douhet's observation still rings true, as demonstrated by the aforementioned attack on the Helmand air base. Indeed, poorly defended air bases will continue to be susceptible to organized ground assaults. Previously, the most successful post-Vietnam air base onslaught occurred during El Salvador's civil war in 1982, in which 100 insurgents attacked an El Salvadoran air force base, destroying five Ouragan aircraft, six UH-1Bs, and three C-47s while damaging five more platforms. Clearly, this "well-planned and executed operation . . . demonstrated the tactical superiority" of the insurgents against the government's base defense force.[3]

Protecting air bases and air and space assets in the future will become exponentially more complex and expensive due to the promulgation of technology, abundance of open-source information, and growth in adversary capabilities. Looking forward, we see that traditional threats such as airborne assault, indirect fire (IDF) through rockets and mortars, and direct attack by suicide squads will continue as staples of enemy action. Consequently, we must examine emerging threats that enable new modes of air base attack, including the development of precision munitions, the spread of remotely piloted vehicles (RPV), the proliferation of shoulder-launched surface-to-air missiles (SAM), an escalating insider threat, and other variants of a new technological bounty for terrorists and insurgents. The defense of air assets will become even more problematic in the face of a spectrum of threats enabled by technology and an accelerating insider threat. This growth and proliferation of technology will enable small groups to gain an even greater advantage against base defenders and air operators.

Certainly, Airmen need to thoughtfully consider the high probability of these emerging threats and the associated costs of ensuring continued operations. Formerly, a man and a rifle filled a gap in a sector of base defense. Well-defended air bases drive the enemy to explore alter-

native means of affecting air operations. Naturally, any rational actor desires the quickest, cheapest route to success after selecting a target. If he does not seek a spectacular attack designed to produce casualties and dramatic television footage (as espoused by groups such as al-Qaeda), then he will likely wish to impede air operations and bleed the base dry through harassment that produces casualties over time.

When examining the threat, however, we must constantly ask ourselves what the enemy will target because it is not necessarily aircraft on the ground. Targets and objectives depend upon the attackers, ranging from terrorist groups to conventional forces to special operations, and upon the political objectives and actual capabilities that they can bring to bear against an air base. In Vietnam, enemy forces found ground attacks against airfields a drain on their resources. As a result, they adapted to disrupt air operations rather than attack airfields directly because "whether the raids resulted in aircraft, facility, or runway damage, sortie rates were impaired. Standoff weapons [IDF in today's parlance], as well as various forms of command-detonated explosives, soon became the weapons of choice amongst the many belligerents engaged in conflict since the 1960s."[4]

The threat of terrorism has driven most base-defense operations to focus on the defeat of vehicle-borne improvised explosive devices (VBIED). Top-tier terrorist groups have long wanted headline-grabbing attacks that are big on visual imagery, shock, and body count. Images of the Marine barracks in Beirut, Lebanon, or the Air Force's Khobar Towers in Khobar, Saudi Arabia, became the adversary's desired outcome of an attack. We see the same intent at play in the Taliban's detonation of a truck bomb on the 10th anniversary of the terrorist attacks of 11 September 2001—a strike that wounded 89 people, including 77 Soldiers.[5] This article examines some of the more alarming threats—such as VBIEDs, which we expect the enemy to use in future attacks—and the emerging technology that could enable him to assail our air bases.

The Growing Precision of Indirect Fire

IDF has become the popular choice among insurgents for attacking an air base. Fired at a distance and often rigged to fire after the attacker has departed, it offers a degree of survivability. In Vietnam, Vietcong and North Vietnamese forces hit American air bases 475 times between 1964 and 1973, primarily with IDF, destroying 99 US and South Vietnamese aircraft and damaging 1,170.[6] In Iraq, insurgents used IDF to harass air bases, but it proved largely ineffective because of a poorly trained enemy and active external base defenses. In Afghanistan the enemy employed IDF not only to harass coalition forces but also to mask and cover ground attacks. On 22 August 2012, enemy forces even managed to damage the visiting aircraft of the chairman of the Joint Chiefs of Staff.[7]

Mortars and rockets, aimed at a base by someone with limited targeting information, rely on the technical expertise of the operator—factors that hinder their overall effectiveness. However, a new age in precision IDF weapon systems is now upon us. On 31 March 2011, Soldiers from the 4th Brigade Combat Team fired a 120 mm precision-guided mortar round from Forward Operating Base Kushamond, Afghanistan, hitting within four meters of the target.[8] Normally a mortar fires a "dumb" round—one that has no onboard guidance system. Over time this technology will likely spread to insurgent and terrorist groups, improving their ability to pick and choose targets with extraordinary accuracy and making aircraft as well as key facilities much more vulnerable.

Defeating this type of weapon system demands a truly integrated technological defense. Both America and Israel have pioneered defensive systems designed to counter the increased precision of IDF weapons. In Iraq, Joint Base Balad and other locations used a jointly manned Counter-Rocket Artillery Mortar system to defend against enemy IDF. The defense establishment will need to ensure a comprehensive defense system in the future because precision rounds will make base attack much simpler and give defending forces less margin for error. Furthermore, the capability of this defense technology is improving.

For instance, during the November 2012 Israeli conflict with Hamas in Gaza, militants launched more than 1,500 rockets at Israel, but that country's Iron Dome, a "portable anti-rocket system built to take down short-range missiles," intercepted about 400 of them.[9] This system may offer a template for a portable defense system for air operations. Should precision IDF rounds become part of the operational environment, our Airmen won't have the luxury of an enemy's incompetent firing of dumb rounds.

Remotely Piloted Vehicles

Personnel contemplating defense of an air base must consider the threat posed by RPVs by formulating a plan to tackle a range of remote threats, both ground and airborne. Who is cleared to engage such vehicles and with what weapons? For ground-based vehicles, the answer is more clearly defined and in line with established contingencies for VBIEDs; however, a defensive gap may exist in defending against airborne threats. The fact that we have yet to fully explore protocols for these defenses leaves a seam that a technologically savvy enemy could exploit. We must develop modeling, simulation, and defenses to account for these new threats before a protest group disrupts flying operations or—worse yet—before a terrorist organization uses RPVs for reconnaissance or attacks against our air assets.

The use of these vehicles (RPVs, robots, drones, etc.) is moving beyond exclusive military use. After all, civilians have flown remote-controlled airplanes since the 1930s. Today, though, the sophistication, range, and video capability allow civilians to access technology once reserved only for military and intelligence organizations. Take the case of a protest group called SHARK (Showing Animals Respect and Kindness). This group planned to use a Mikrokopter drone to videotape a live pigeon shoot as a means of deterring and interfering with a legal hunting outing. On 21 February 2012, SHARK set up operations at Broxton Bridge Plantation near Ehrhardt, South Carolina. Law enforcement officers and a local attorney tried to prevent the protest

group from flying its drone, but the group flew anyway, only to have the drone shot down by hunters on the scene.[10]

This same technology is capable of carrying weapons or conducting reconnaissance for groups targeting an airfield—indeed, it has already done so. For example, although American policy makers have concerned themselves with al-Qaeda in recent years, Hezbollah has proven itself to have global reach and staying power. It is credited as the first terrorist group to pioneer the use of suicide bombers as a weapon of mass destruction, delivering large vehicle bombs to specific targets.[11] Hezbollah has recently shown technological prowess through its use of explosive-laden RPVs and missile technology, even managing to cripple an Israeli warship.[12] The success of the organization comes from its financial and logistical backing by Syria and Iran, the latter supplying advanced weapons and reconnaissance equipment.

Starting in November 2004, Hezbollah shocked Israelis by launching a remotely piloted surveillance plane, the Mirsad 1, that flew over Israeli towns and returned to Lebanon unharmed. At a Hezbollah rally, the organization's leader, Hassan Nasrallah, declared, "You can load the Mirsad plane with a quantity of explosive ranging from 40 to 50 kilos and send it to its target. . . . Do you want a power plant, water plant, military base? Anything!"[13] No doubt this technology will spread to other terrorist and protest groups over time.

To punctuate this point, examine the case of Rezwan Ferdaus, a 26-year-old US citizen. He was arrested on 28 September 2011, charged with plotting to attack the Pentagon and US Capitol with "large remote controlled aircraft filled with C-4 plastic explosives" and providing "material support and resources to a foreign terrorist organization, specifically to al Qaeda."[14] According to the Federal Bureau of Investigation, Ferdaus planned to couple his "aerial assault" by three explosive-laden drones with a ground attack that included "six people, armed with automatic firearms and divided into two teams." Ferdaus explained that "with this aerial assault, we can effectively eliminate key locations of the P-building [Pentagon] then we can add to it in order to take out

everything else and leave one area only as a squeeze where the individuals will be isolated, they'll be vulnerable and we can dominate."[15]

Proliferation of Shoulder-Launched Surface-to-Air Missiles

A flying wing can realize mission success only by generating aircraft sorties, regardless of threats from the operational environment. Protecting aircraft from SAMs during takeoff, the most vulnerable phase of flight, is extremely challenging due to constraints on their maneuverability caused by weight and low altitude. Consequently, heavy transport aircraft and their valuable cargo, possibly munitions and/or passengers, present extremely tempting targets during takeoff. Conversely, aircraft on approach must maintain predictable speeds and flight paths. In either case, SAMs represent a threat to such aircraft. For instance, rebels in the current Syrian conflict allegedly possess some "fifteen to thirty SA-7 man-portable air-defense systems [MANPADS]" and have "reportedly shot down at least five rotary-wing and six fixed-wing aircraft," claiming at least one downed by a MANPADS.[16] According to the US Air Force Counterproliferation Center,

> Currently, 27 terrorist groups including Al Qaeda have confirmed or reported possession of MANPADS. Since 1994, there have been ten high profile attempts to target commercial aircraft with four being shot down—including one carrying the Presidents of Rwanda and Burundi. Furthermore, MANPADS fit Al Qaeda's mode of operation perfectly and are relatively easy to use, convenient to transport, widely available, inexpensive, and certainly lethal.[17]

As technologies developed by foreign competitors continue to advance and proliferate, tactics, techniques, and procedures for integrated defense will have to keep up with their employment. Recently the Russian-made SA-24 "Grinch" MANPADS proliferated to Venezuela, Libya, and Syria.[18] Of course, Libya's government has been deposed, and at this writing Syria remains in a state of civil war. The security of MANPADS in such war-strewn countries remains doubtful as potential black markets develop and instability attracts nefarious elements. The

threat of MANPADS to future US and coalition forces as well as civilian airline operations will likely rise as these systems become more accessible in the fertile ground of civil war and insurgency.

The Expanding "Insider Threat"

For the foreseeable future, US and coalition forces will operate amid insider threats. In Afghanistan from 2007 to 2011, Pentagon statistics reveal a total of 42 attacks by members of the Afghan National Security Forces on US and NATO personnel, claiming the lives of 70 coalition troops and wounding 110 others.[19] One of the most egregious and horrific instances of an insider threat occurred on the morning of 27 April 2011, when an Afghan air force captain killed eight Airmen and one contractor at Kabul International Airport.[20] Another incident demonstrated how a determined and crafty suicide bomber could infiltrate a Central Intelligence Agency base in eastern Afghanistan and kill eight Americans.[21] This disturbing trend intensified in 2012 as uniformed Afghan security forces conducted 46 insider attacks against coalition forces, which killed 60 NATO personnel.[22]

More troubling still is the growing threat from within the ranks of American personnel. On 11 May 2009, five American military members were killed by a US Soldier at a military counseling center in Camp Liberty, Baghdad.[23] Shootings by a US Army psychiatrist on 5 November 2009 in Fort Hood, Texas, resulted in the deaths of 13 people and wounding of 32 others.[24] Clearly, the Department of Homeland Security is concerned about the threat that veterans could mount in the homeland, noting that veterans returning from Iraq and Afghanistan could be susceptible to recruitment by right-wing extremists.[25]

It is important to remember that one person can do a great deal of harm—witness the number of "lone wolf" incidents that have occurred. On 22 July 2011, for example, Anders Breivik, a Norwegian, set off a vehicle bomb near government buildings in Oslo, killing eight, and then massacred 69 people at a youth camp on the nearby island of

Utoeya.[26] On 20 July 2012, American James Holmes walked into a sold-out movie theater near Denver and began shooting; he killed 12 and wounded 58.[27] Trained and experienced US military members and veterans could wreak even more havoc. Whether stateside or overseas, commanders must ensure that they provide and exercise a comprehensive interior security plan—one that includes an aggressive psychological screening program to identify insider threats.

Obtaining Maps of Air Bases

Enemy forces planning a ground assault of an air base used to rely on collaborators who had access to the target base to facilitate the mapping of terrain and key facilities, as well as attain pace counts that enable IDF attacks. Today the information superhighway offers access to satellite imagery and other open-source information that make the job of a would-be attacker much easier. One such website, that of the Federation of American Scientists (FAS), describes itself as "an independent, nonpartisan think tank and registered 501(c)(3) non-profit membership organization . . . dedicated to providing rigorous, objective, evidence-based analysis and practical policy recommendations on national and international security issues connected to applied science and technology."[28] GlobalSecurity.org, an offshoot of FAS founded by John Pike, one of its former members, claims to be "the leading source of background information and developing news stories in the fields of defense, space, intelligence, WMD [weapons of mass destruction], and homeland security."[29] Its website features satellite images of military bases around the world, many of which the US government considers classified. Other sites, such as Google Maps, make available imagery and street maps. In sum, people now have a multitude of ways to acquire detailed maps of air bases that would facilitate attacks on those locations.

Social Media: Flash Mobs, Terrorism, and Networking Base Attacks

Instantaneous communications will dramatically improve the enemy's information operations and base attacks, allowing him to draw upon elements of a sympathetic local populace to create situations that embarrass an air base's leadership or overwhelm defenses. Thus, intelligence and law enforcement must stay one step ahead of an increasingly agile foe by becoming more adept in their collection efforts. Basic technology, such as cell phones, has affected society in unusual ways by creating unprecedented means for communicating and coordinating actions. Take for example the phenomenon of the "flash mob," a group of people summoned via cell phone, social media, and viral e-mails for the purpose of performing some sort of act at a specific location. The web and even commercials of telecommunications companies are replete with footage of benign flash mobs who appear in a public place to carry out some sort of unusual or artistic act, like freezing in one place or performing a coordinated dance routine. Although they do this in the name of entertainment, what happens when someone uses this same technology for nefarious purposes?

In the summer of 2011, for example, Philadelphia was hit with an epidemic of flash mobs organized to carry out robberies, assaults, looting, and chaos. This incident included random beatings of pedestrians, a rampage through a Sears store, and assemblages of hundreds of people at designated locations designed to choke traffic. Margaret Rock, editor at Multimedia.com in Chicago, offered the following: "I don't know why, but what started out as something used for good has shown its dark side."[30] Later that same summer, riots in London, Birmingham, Manchester, and elsewhere developed, causing security officials great concern. Scotland Yard identified and arrested nearly 3,000 people suspected of physically rioting or inciting violence across the country by using BlackBerry Messenger, Twitter, and Facebook.[31] According to one text, "If you're down for making money, we're about to go hard in east London."[32] David Cameron, British prime minister, observed that "every-

one watching these horrific actions will be struck by how they were organized via social media. . . . So we are working with the police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality."[33]

The rapid pace of technological advancement has spread to every corner of the globe. Cell phones are now powerful computers in their own right, networking with other devices globally. Nowhere is this more apparent than in developing countries that had poor communications because of the cost of hard-wiring infrastructure for land lines. Cell phones now make that expense moot since towers and satellites allow such countries to plug into the global communications grid. As of 2008, 80 percent of the world's population had access to a cellular network, and by the end of 2006, developing countries bought 68 percent of the world's mobile phones.[34]

The same technology that enables global information sharing and advancement also supports the networking of terrorist and criminal groups. According to a new study by Israel's University of Haifa, al-Qaeda, Hamas, Hezbollah, and the like have invested in social networking such as Facebook and Twitter to recruit, raise funds, and gather intelligence. Prof. Gabriel Weimann, author of the study, argues that "today, about 90 per cent of organized terrorism on the internet is being carried out through social media" and that the latter is "enabling the terror organizations to take initiatives by making 'friend' requests, uploading video clips and the like and they no longer have to make do with the passive tools available on regular websites."[35]

How will this technology and social networking affect base security in the future? Protestors, mobs, and terrorist groups could easily be summoned with no prior notice to military intelligence or law enforcement, quickly assembling near a base's entry-control point or perimeter to protest, riot, or attack. In many instances, such areas would have only a handful of guards available to counter the assembled

groups—a scenario that could easily overwhelm the few personnel on scene and escalate beyond their capacity to quell such action.

Cyber Attacks: A Potential "Easy Button" for Air Base Attack

Technological advances have pushed the US military into a "cyber force" largely dependent upon a network of computers and communications links to ensure not only the effective use of forces during contingency operations but also the day-to-day mission of force preparation and training. Thus far, insurgent forces have lacked the capability and training to conduct large-scale cyber attacks against military installations. However, that will likely change as state-sponsored terrorist organizations and insurgent forces partner to defeat a common enemy. Utilizing a cyber attack that affects air operations or base-defense sensors and cameras to facilitate a kinetic strike may be a cost-effective and efficient choice.

Attacks via cyberspace could result in degraded flight operations, as occurred at the Indira Gandhi International Airport when a malicious code, utilizing scripts specifically designed to exploit that system's weakness, shut down check-in counters and boarding gates and significantly affected operations.[36] A similar assault could disrupt air-traffic-control nodes, networked maintenance schedules, and training operations as well as threaten armed or unarmed RPVs operated by the Air Force and other government agencies. Take for example the recent hacking of a Department of Homeland Security drone as part of a bet between a Texas college professor and his students. For less than $1,000, these individuals successfully "spoofed" the RPV, effectively "re-missioning" it.[37] This low-budget academic prank demonstrates how easily an adversary or terrorist group could re-mission RPVs and turn them into flying missiles against an air base or other target.

Red Flag, the Air Force's combat-training exercise involving US and allied forces, has integrated cyber and space elements from Air Force

Space Command to address effects associated with attacks on cyber and space assets. At the March 2011 Red Flag, an Air Force official commented, "We know many threats around the world are working diligently to access, corrupt, or deny our use of [both unclassified and classified computer systems]."[38] Assets and personnel associated with integrated defense systems may also become targets. Further, adversaries might try to disrupt or manipulate the increasing use of cyberspace for communications, including encrypted radio transmissions, classified and unclassified messaging, and biometric identification systems at our access gates. A *Washington Post* investigation found that certain types of software platforms used by government and the private sector—including a Tridium company system called Niagara—are more vulnerable than others. Marc Petock, Tridium's vice president for global marketing and communications, noted that "some Defense Department facilities in the United States also depend on Niagara. That includes the giant Tobyhanna Army Depot in Pennsylvania" and some "high security" military facilities.[39]

The rapidly evolving cyber domain promises many benefits: reduced manpower requirements, increased efficiency, better targeting, and ease of access/use. However, these same technologies present significant opportunities for a clever and determined adversary to create a backdoor through which he can penetrate and defeat the entire security system.

Marrying Modern Technology with Special Forces

Not too long ago, planners at NATO bases concentrated on the USSR's plans to attack air bases. During the Cold War, the Soviets explored a number of ways to assault and disable bases, primarily by employing the Spetsnaz (special forces). A review of Spetsnaz airfield-attack profiles in declassified Cold War–era Central Intelligence Agency reports would prove useful because they provide insights into methods for direct strikes on these targets. These included the airdrop near an air base of 30 special operators, who then broke into "four operations

teams, each team with specific responsibilities including capturing vehicles and personnel for the purpose of infiltrating the target [air base]," using SAMs and explosive devices to destroy aircraft.[40] Additionally,

> in a second method, a Spetsnaz company (approximately 10 teams of five to 12 men) operated against a heavily defended airfield. The company could not get closer than 2 to 3 km to the target. During the first night Block Strelas [three-tubed SAM launchers mounted on a tripod] were positioned as close as possible to either end of the field, and then attacks were initiated against pipelines, powerlines, communication lines, security personnel, and crews heading toward the airfield.[41]

This would disrupt airfield operations, create the impression that a larger Soviet force was in the area, and draw more NATO forces in for defense and away from the front lines. Imagine well-trained enemy special forces enabled by many of the aforementioned technological advances. Base defense would become incredibly difficult, and the complexity of countering the threat would escalate significantly.

Conclusion

Understanding and countering these growing threats will play a major role in the ability to project airpower effectively in the future. One solution—basing aircraft as far from hostilities as possible—strains aircraft and aircrews with longer flight times. However, it does not address the likely requirement that mobility aircraft land near or in the combat zone to support ground operations. Nor does remote basing speak to the technological means of attack through cyberspace, technologically enabled terrorists, or special forces hitting a presumably safe air base. Thus Airmen must conduct a truly full-spectrum threat analysis and take into account these potential vulnerabilities in force-protection planning.

Aircraft are extremely fragile. One well-placed mortar round can render several hundred million dollars' worth of aircraft worthless or can wipe out a barracks occupied by essential personnel such as pilots or aircraft technicians. The Air Force and coalition forces will have to

make hard choices about base defense driven by mission requirements, economic constraints, and the rising threat posed by a determined enemy enabled by some of the aforementioned technology. Airmen and joint leaders must either stay abreast of these issues during the interwar period or risk the elimination and degradation of air assets at the onset of the next hard-fought campaign. ✪

Notes

1. Barbara Starr, Chris Lawrence and Joe Sterling , "ISAF: Insurgents in Deadly Attack in Afghanistan Wore U.S. Army Uniforms," Cable News Network , 15 September 2012, http://www.cnn.com/2012/09/14/world/asia/afghanistan-fatal-attack/index.html.

2. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of Air Force History, 1983), 53–54.

3. James S. Corum and Wray R. Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists* (Lawrence: University Press of Kansas, 2003), 334–35.

4. Maj Michael P. Buonaugurio, USAF, "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision" (master's thesis, Marine Corps Command and Staff College, 2001), 8, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA401262.

5. Jeremy Kelly, "NATO Military Base Attacked by Suicide Bomber in Afghanistan," *Guardian*, 11 September 2011, http://www.guardian.co.uk/world/2011/sep/11/us-base-suicide-bomber-afghanistan.

6. Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases* (Santa Monica, CA: RAND, 1995), 68, http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR553.pdf.

7. Barbara Starr, "Shrapnel Hits Joint Chiefs Chairman's Plane at Afghan Base" Cable News Network, 21 August 2012, http://articles.cnn.com/2012-08-21/asia/world_asia_afghanistan-dempsey-plane_1_fight-against-afghan-green-on-blue-afghan-man-afghanistan.

8. SSgt Todd Christopherson, "Soldiers Fire First Precision-Guided Mortar in Afghanistan," US Army, 7 April 2011, http://www.army.mil/article/54502/.

9. Jennifer Rizzo, "U.S. Continues Support for Israel's Iron Dome," Cable News Network, 17 May 2012, http://articles.cnn.com/2012-05-17/us/us_israel-missile-system_1_anti-rocket-iron-dome-missile-defense?_s=PM:US; and Ernesto Londoño, "For Israel, Iron Dome Missile Defense System Represents Breakthrough," *Washington Post*, 2 December 2012, http://www.washingtonpost.com/world/national-security/for-israel-iron-dome-missile-defense-system-represents-breakthrough/2012/12/01/24c3dc26-3b32-11e2-8a97-363b0f9a0ab3_story_1.html.

10. Rebecca Boyle, "After Animal Activists Track Pigeon Hunt with Drone, Pigeon Hunters Shoot Down Drone," *Popular Science*, 21 February 2012, http://www.popsci.com/technology/article/2012-02/after-pigeon-hunt-thwarted-shooters-take-down-activist-groups-spy-drone.

11. Capt Daniel Helmer, "Hezbollah's Employment of Suicide Bombing during the 1980s: The Theological, Political, and Operational Development of a New Tactic," *Military Review*, July–August 2006, http://www.army.mil/professionalWriting/volumes/volume4/november_2006/11_06_1.html.

12. Associated Press, "Israel: Iranian Troops Helping Hezbollah Attack," *NBC News*, 16 July 2006, http://www.nbcnews.com/id/13875121/.

13. Lisa Myers, "Hezbollah Drone Threatens Israel," *NBC News*, 12 April 2005, http://www.msnbc.msn.com/id/7477528/ns/nbcnightlynews/t/hezbollah-drone-threatens-israel/.

14. "Massachusetts Man Charged with Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Material Support to a Foreign Terrorist Organization," press release, Federal Bureau of Investigation, 28 September 2011, http://www.fbi.gov/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization.

15. Ibid.

16. Eddie Boxx and Jeffrey White, "Responding to Assad's Use of Airpower in Syria," Washington Institute for Near East Policy, 20 November 2012, http://www.washingtoninstitute.org/policy-analysis/view/responding-to-assads-use-of-airpower-in-syria.

17. James C. "Chris" Whitmire, *Shoulder Launched Missiles (a.k.a. MANPADS): The Ominous Threat to Commercial Aviation*, Counterproliferation Papers, Future Warfare Series no. 37 (Maxwell AFB, AL: USAF Counterproliferation Center, Air University, December 2006), 1, http://cpc.au.af.mil/PDF/monograph/manpads.pdf.

18. David Fulghum and Robert Wall, "Russia's SA-24 'Grinch' Lands in Insurgent Hands," *Aviation Week and Space Technology*, 12 March 2012, http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_03_12_2012_p27-433282.xml&p=1.

19. Anna Mulrine, "Taliban Infiltrators in Afghanistan? Pentagon Warns of 'Insider Threat,' " *Christian Science Monitor*, 1 February 2012, http://www.csmonitor.com/USA/Military/2012/0201/Taliban-infiltrators-in-Afghanistan-Pentagon-warns-of-insider-threat.

20. Jill Laster, "Motive in Kabul Shooting Deaths Remains Elusive," *Air Force Times*, 17 January 2012, http://www.airforcetimes.com/news/2012/01/air-force-motive-in-kabul-shooting-deaths-remains-elusive-011712/.

21. Joby Warrick, "Suicide Bomber Attacks CIA Base in Afghanistan, Killing at Least 8 Americans," *Washington Post*, 31 December 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/12/30/AR2009123000201.html.

22. "What Lies behind Afghanistan's Insider Attacks?," British Broadcasting Corporation, 11 March 2013, http://www.bbc.co.uk/news/world-asia-19633418.

23. Timothy Williams, "U.S. Soldier Kills 5 of His Comrades in Iraq," *New York Times*, 11 May 2009, http://www.nytimes.com/2009/05/12/world/middleeast/12iraq.html?_r=2.

24. Joseph I. Lieberman and Susan M. Collins, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, special report (Washington, DC: US Senate Committee on Homeland Security and Governmental Affairs, February 2011), http://www.hsgac.senate.gov/download/fort-hood-report.

25. Associated Press, "Homeland Security Leaders Defend Memo on Veterans," *USA Today*, 19 April 2009, http://usatoday30.usatoday.com/news/washington/2009-04-19-homeland-memo_N.htm.

26. "Anders Breivik Describes Norway Island Massacre," BBC, 20 April 2012, http://www.bbc.co.uk/news/world-europe-17789206.

27. M. Alex Johnson and Pete Williams, "Cops: Weeks of Planning Went into Shootings at Colo. Batman Screening," *NBC News*, 20 July 2012.

28. "About FAS," Federation of American Scientists, accessed 29 January 2013, https://www.fas.org/about/index.html.

29. "Company History," GlobalSecurity.org, accessed 13 March 2013, http://www.globalsecurity.org/org/overview/history.htm.

30. John Timpane, "Flash-Mob Violence Raises Weighty Questions," Philly.com, 14 August 2011, http://articles.philly.com/2011-08-14/news/29886718_1_social-media-flash-mob-facebook-and-other-services.

31. Neil Lancefield, "3,000 Arrests in London Riots Investigation," *Independent*, 7 October 2011, http://www.independent.co.uk/news/uk/crime/3000-arrests-in-london-riots-investigation-2366933.html.

32. Timpane, "Flash-Mob Violence."

33. Josh Halliday, "David Cameron Considers Banning Suspected Rioters from Social Media," *Guardian*, 11 August 2011, http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media.

34. Sara Corbett, "Can the Cellphone Help End Global Poverty?," *New York Times*, 13 April 2008, http://www.nytimes.com/2008/04/13/magazine/13anthropology-t.html?pagewanted=all.

35. "Terrorist Groups Recruiting through Social Media," Canadian Broadcasting Corporation News, 10 January 2012, http://www.cbc.ca/news/technology/story/2012/01/10/tech-terrorist-social-media.html.

36. Rahul Tripathi, "Cyber Attack Led to IGI Shutdown," *Indian Express,* 25 September 2011, http://www.indianexpress.com/news/cyber-attack-led-to-igi-shutdown/851365/.

37. "Texas College Hacks Government Drone in Front of DHS," Autonomous Nonprofit Organization ("TV-Novosti"), 27 June 2012, http://rt.com/usa/news/texas-1000-us-government-906/.

38. TSgt Scott McNabb, "Red Flag Cyber Operations: Part I—Isn't Red Flag a Flyer's Exercise?," Air Force Space Command, 1 March 2011, http://www.afspc.af.mil/news/story.asp?id=123244481.

39. Robert O'Harrow Jr., "Tridium's Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks," *Washington Post*, 11 July 2012, http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html.

40. Director of Central Intelligence, *Warsaw Pact Nonnuclear Threat to NATO Airbases in Central Europe*, NIE 11/20-6-84, 25 October 1984, 35, http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000278545.pdf. Document is now declassified.

41. Ibid., 36, 39.

Col Shannon W. Caudill, USAF

Colonel Caudill (BS, Norwich University; MS, Central Michigan University; MMS, Marine Corps University) is a student in the Air War College's Grand Strategy Program and the former deputy chairman of the Department of Leadership and Strategy, Air Command and Staff College, Maxwell AFB, Alabama. Prior to his current assignment, he commanded the 532nd Expeditionary Security Forces Squadron (the Lions), Joint Base Balad, Iraq. As a career Air Force security forces officer, he has worked at the unit, major command, and Joint Staff levels; commanded three security forces squadrons; served in four overseas assignments; and accumulated 18 months of combat experience in Iraq. Colonel Caudill has written numerous white papers and articles on terrorism, interagency leadership, and law enforcement, which have appeared in *Air and Space Power Journal*, *Joint Force Quarterly*, *American Diplomacy*, and *The Guardian*—the Joint Staff's antiterrorism publication. He is a graduate of Squadron Officer School, Marine Corps Command and Staff College, and Joint Forces Staff College.

Maj Benjamin R. Jacobson, USAF

Major Jacobson (BS, University of Idaho; MBA [Criminal Justice emphasis], Touro University; MMOAS, Air Command and Staff College) is the deputy course director of the Air, Space, and Cyber Power Studies Course, Department of Leadership and Strategy, Air Command and Staff College, Maxwell AFB, Alabama. Prior to his current assignment, he commanded the 96th Ground Combat Training Squadron, Eglin AFB, Florida. As a career Air Force security forces officer, he has worked at the unit, wing, and major command levels and served in two overseas assignments. Major Jacobson is a graduate of the Aerospace Basic Course, Squadron Officer School, and Air Command and Staff College.

Let us know what you think! Leave a comment!